Understanding the Enhanced Mitigation Experience Toolkit

Frequently Asked Questions[1]

MIT-001FQ-2014
MITIGATIONS GUIDE - FAQ
OCTOBER 2014

1 Revision Statement: IAD Technical Report "Understanding the Enhanced Mitigation Experience Toolkit Frequently Asked Questions", dated October 2014 replaces the previous version entitled "Microsoft's Enhanced Mitigation Experience Toolkit A Rationale for Enabling Modern Anti-Exploitation Mitigations in Windows Frequently Asked Questions." The previous FAQ document and the replacement contain identical content. The document name was changed to assist in providing a distinction to a similar document entitled "Microsoft's Enhanced Mitigation Experience Toolkit A Rationale for Enabling Modern Anti-Exploitation Mitigations in Windows" that did not have the FAQ appended to the title.

Microsoft®'s Enhanced Mitigation Experience Toolkit (EMET) is an enhancement to the Windows® operating system that stops broad classes of malware from executing. EMET implements a set of anti-exploitation mitigations that prevent the successful exploitation of memory corruption vulnerabilities in software, including many zero-day and buffer overflow attacks. EMET inhibits many of the attacks currently used by Advanced Persistent Threat (APT) actors. EMET provides significant software protection for all currently supported versions of the Windows operating system, supports enterprise deployment, configuration, and event forwarding (an additional threat analytic source).

Background

Who should read this document?

This document should be read by technical managers, security officers, administrators, and cyber defenders who are unfamiliar with Microsoft's Enhanced Mitigation Experience Toolkit (EMET). The document is presented as a list of Frequently Asked Questions (FAQs).

What is Microsoft's EMET?

EMET is an enhancement to the Windows operating system that stops broad classes of malware from executing. EMET is as easy to install as a "patch."

How much does EMET cost? What is the license fee?

EMET is freely available from Microsoft without material cost.

Does EMET require significant resources to maintain and manage?

Although EMET is provided without cost by Microsoft, an organization must commit some level of trained manpower and resources to configure, test, and install EMET. Thereafter, maintenance cost is nominal: an organization should monitor "EMET alerts." This activity can be integrated into the organization's existing network defense operations. While EMET alerts can be ignored, the organization will lose a valuable source of threat information.

Simply, how does EMET stop malware?

Attackers use the web, email, and other tricks to convince a user to open a Word, Excel, PowerPoint, PDF, and other documents. Once opened, the improperly formatted file causes the computer to run code (the attacker's program) inside the file. EMET inhibits (malicious) code from running inside a data file.

Is EMET required?

Yes. The Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) requires EMET version 3.0 or later. (1)(2)(3) Reference vulnerability identifiers: V-36701, V-36702, V-36703, V-36704, V-36705, and V-36706.

Purpose

Why is EMET important? What does EMET do for my organization?
EMET stops many forms of malware from running, and prevents data exfiltration, data theft, and the theft of personally identifiable information (PII) resulting from the installation of malware.

What threat is EMET designed to stop?
EMET counters a variety of "infection vectors," including malware sent to you in an email or sent from the web. EMET inhibits attacks currently used by Advanced Persistent Threat (APT) actors.

Is EMET effective?
Yes. EMET provides advanced security mitigations to protect software from zero-day, buffer overflow, and other memory corruption attacks. EMET stops the majority of cyber attacks in use today. However, EMET is not a panacea. World-class hackers are trying very hard to circumvent EMET protected systems, and fringe exploits to counteract EMET are emerging. These truly sophisticated exploits may become mainstream in 1-2 years. However, running without EMET protections makes your system an easy target.

Compatibility Concerns

Which version of Windows is compatible with EMET?
EMET works on XP, Vista, Windows 7, and Windows 8. Not all mitigations are available in every version of Windows.

Does EMET work with the Host Based Security System (HBSS)?
Yes. EMET is compatible with HBSS. Specifically, EMET version 4.1 is fully compatible with HBSS Host Intrusion Protection System (HIPS) 8.0 patch 4. For other versions of EMET and HBSS HIPS, "Deep Hooks," an advanced mitigation appearing in EMET version 4.0, must be disabled to maintain compatibility with HIPS prior to patch 4:

EMET version	"Deep Hooks" mitigation	HBSS HIPS	Compatible
3.0	Deep Hooks not available	All versions	Yes
4.0	Deep Hooks is introduced and Enabled by default	Prior to patch 4	Yes, disable "Deep Hooks"
		Patch 4	Yes, disable "Deep Hooks"
4.1	Disabled by default during installation	Prior to patch 4	Yes
		Patch 4	Yes, enable "Deep Hooks"
4.1 Update 1	Enabled by default during installation	Prior to patch 4	Yes, disable "Deep Hooks"
		Patch 4	Yes

Although EMET version 3.0 is compatible with all versions of HBSS, EMET version 3.0 does not offer the newest mitigations, and is not preferred.

Is EMET compatible with my browser and other office automation software?
Yes, with limited exceptions (e.g., some browser plug-ins). In these instances, the conflicting EMET mitigation should be disabled for the offending application. The remaining mitigations will still be enforced on that application and compatibility maintained.

Will EMET impact my mission critical, custom, or legacy application?

This is an important concern: Microsoft indicates that incompatibilities with EMET should be limited to applications which dynamically generate code, such as a Just-In-Time (JIT) compiler, and certain drivers that do not explicitly mark generated code in a data section with the execute permission. In all cases, critical, custom, and legacy applications should be tested. EMET can be configured to "opt-out" mission critical applications, and will not impact those applications. The majority of malware targets the most common user programs, including Microsoft Office applications, Internet Explorer, Adobe Reader and Flash, Java, and Mozilla; EMET protection of these applications provides the greatest return, even if custom programs are opted-out.

Does "application whitelisting" interfere with EMET?

No. EMET, application whitelisting, and the organization's antivirus software are used in conjunction and as part of a host mitigation package. EMET prevents system exploitation. Application whitelisting restricts execution to approved applications. Antivirus software detects malicious content.

Are some applications incompatible with the mitigations provided by EMET?

There are a few applications that are incompatible with some of EMET's protections. These applications are well known, and profiles to "opt-out" those incompatibilities are available in the EMET distribution.

Installation, Versions, and Alternatives

Is EMET easy to install?

Yes. Administrators can use Active Directory, specifically "group policy," to deploy EMET in large organizations (e.g., thousands or hundreds of thousands of systems). Large organizations normally have Active Directory, and the time required for installation is typically a few hours. For small organizations, an administrator can use the manual installer.

Is there a system prerequisite for installation?

Yes. EMET requires .NET for installation. The minimal version of .NET varies for different versions of EMET.

Does EMET require formal training for installation?

No. EMET is as easy to install as a "patch." Microsoft provides a few pages of screen shots to complete an installation.

Are there alternative anti-exploitation tools for Windows?

Yes. An administrator may enable DEP, ASLR, and SEHOP by manually configuring entries in the control panel, system registry, and Image File Execution Option (IFEO) keys. However, configuration via these three lower level mechanisms is more complex than using EMET's single interface. EMET also has additional mitigations, beyond those found in the Windows operating system. Researchers are also developing anti-mitigation prototypes that may not be ready for enterprise deployment.

Our organization already installed EMET. Can we easily install a new version?

Yes. An administrator should uninstall the older version of EMET, remove two registry hives, and then install the new version. See the Microsoft EMET User Guide.

User's Experience and Expectation

On a day-to-day basis, what can I expect from EMET?

EMET will not interfere with a user's work environment or add any significant processing requirements. EMET does not run any long-duration system scans. EMET does not affect the user's perceived speed of the system.

What does the user see when EMET stops malware?

EMET will terminate execution of the application under attack and present a popup on the user's screen. Users should be advised to submit a ticket for the alert. EMET will additionally write a log message to the Windows Event Log.

OK, a "popup alert and an EMET log message" is too much trouble.

Users may ignore the EMET popup alert since the malware did not exploit the system, but the organization will lose important insight if the alert is not reported or logged. Additionally, if users are not informed about the popup, they may attempt to re-open the malicious file and receive the same EMET popup. This is confusing. Users should be made aware that if they receive an EMET alert, it likely means that the file they were opening (or site they were visiting, etc.) was infected with malware.

Does EMET require regular administrative intervention?

No. After installing EMET and configuring which applications are protected, EMET does not require any additional intervention. An administrator should investigate EMET alerts generated on a user's system to identify the malware. An administrator should also ensure that EMET protections are enabled for any newly added software.

Technical

What type of "security mitigation" is EMET? What would I call EMET?

EMET is a type of "anti-exploitation tool." More familiar mitigation techniques include: antivirus products, host-based protection, intrusion detection systems, patching, etc. Anti-exploitation measures are not new; EMET enables the anti-exploitation measures within Windows.

Specifically, what defensive mitigations does EMET use to stop malware?

EMET forces applications to use several key mitigations built into Windows including Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), and Structured Exception Handler Overwrite Protection (SEHOP). DEP prevents data from executing and ASLR prevents malware from assembling its malicious activity from (multiple and specific) memory locations assigned in the system's memory. SEHOP prevents malware from overwriting entries in the structured event handler and malicious code referenced by that entry. EMET version 4.1 includes other mitigations beyond DEP, ASLR, and SEHOP, the three principal security mitigations.

Does EMET require significant system resources (memory or CPU cycles)?

No. Microsoft asserts that EMET is highly optimized and induces no noticeable overhead on protected applications (4). EMET operates as an extremely small check that verifies where code executes, to ensure that data is not executed like code.

Our expert says that Windows already incorporates "EMET mitigations."

Correct. Many of EMET's mitigations are built into the Windows operating system and are already used by some applications. However, many developers do not activate these built-in Windows protections for their applications. EMET enables the built-in security mitigations for any application. Additionally, EMET adds additional protections that are not integrated into older versions of Windows.

Since EMET enables "built-in" mitigations, why isn't EMET just built-in?

Security mitigations within the operating system are achieved in a patch-work fashion and are not easily enabled for all applications. EMET centralizes the management of these mitigations, adds them to legacy versions of Windows when possible, facilitates their activation, and simplifies their control on each application. EMET has additional mitigations that are outside of the operating system.

Our expert will want to know exactly which protections are enabled by EMET.

An administrator can use EMET's graphical interface to visually inspect which security mitigations are enabled for each application, if desired.

Does EMET produce false positives?

Maybe. If an organization has custom applications that rely on obscure memory manipulations that produce executable data, then EMET will abort the application and produce an alert. In this instance, the organization sees a false positive. Organizations should enable EMET, and then test their custom applications before deployment. Alternatively, an organization can enable EMET (choose "opt-out") and then disable specific mitigations on applications blocked by EMET.

I know that EMET cannot be perfect. What does EMET not do?

EMET does not prevent users from running a Trojan program. If the user is tricked into "double-clicking" on a screen saver (an executable), that Trojan runs with the privilege and access to the files of the user. The Trojan can then install malicious software, even if EMET is installed. Application whitelisting prevents this threat (i.e., unknown programs from executing).

Is Microsoft actively improving EMET?

Yes. Microsoft actively upgrades EMET when new security mitigations become available. As of July 2014, EMET version 5.0 is the current enterprise-deployable version. Microsoft typically releases one version a year. (Microsoft announced EMET version 1.0 in 2009.)

Is EMET better than my antivirus software?

EMET is not a substitution for antivirus software. Antivirus software detects the presence of malware after the malware is installed on the system. EMET prevents the malware from getting onto the system in the first place. EMET and your antivirus software are used together.

I have heard about root kits. What does EMET do regarding root kits?

EMET is an anti-exploitation tool that stops data files from running, including malware that would install a root kit.

Does EMET remove malware that is already on my system?

No. EMET is not a malware removal tool. Microsoft has a Malicious Software Removal Tool for that purpose.

Does EMET require regular updates?

EMET does not require regular updates. EMET does not use "signature files." Although many security products, for instance antivirus software and intrusion detection rules, require regular updates, EMET's security mitigations do not change after installation. If Microsoft releases a new version of EMET, an administrator may choose to install that new version of EMET to keep their system current.

Do I still need to patch my system and run Windows Update?

Yes. System updates and other patches from various software vendors will still be installed as per good security practice. In many instances, EMET protections will prevent exploitation of an un-patched application. EMET should not be used as a rationale to neglect organizational software updates.

Our organization patches our applications regularly. Is EMET really needed?

Yes. New vulnerabilities are discovered in system and application libraries that may not be patched by any vendor. EMET will protect these application components from memory corruption attacks.

Simply, how can our organization test EMET?

EMET can be configured to operate in "Audit Mode". In this mode, EMET does not terminate a program when a memory corruption event is detected. EMET will report the event, and anomalous compatibility issues can be resolved in this mode.

Does EMET report information back to Microsoft?

By default, EMET version 4.0 and 4.1 sends information back to Microsoft. However, EMET's participation in Microsoft's Early Warning Program can be disabled from the "Reporting" menu, or configured to use System Center Agentless monitoring to forward data to the organization's server.

Can specific users have different EMET profiles and different protections?

While it is likely that some users will have access to specific applications, EMET utilizes a single protection profile on the system.

Does EMET integrate into my event forwarding logs?

Yes. When EMET stops an application from executing data, EMET writes to the event log. EMET's event log can be integrated into the organization's network defense processes.

Does EMET work in a Virtual Machine (VM)?

Yes with limitations. Refer to the Microsoft EMET User Guide.

Where can our organization obtain a copy of EMET?

EMET version 4.1 update 1 is located on the following page:

http://www.microsoft.com/en-us/download/details.aspx?id=41138

EMET version 5.0 is located on the following page:

http://www.microsoft.com/en-us/download/details.aspx?id=43714

The supported lifecycle dates for EMET are located at:

http://support.microsoft.com/kb/2458544

References

1. Windows XP® Security Technical Implementation Guide Overview, Version 6, Release 1.29. s.l. : Field Security Operations, Defense Information Systems Agency, 26 Jul 13.
2. Windows 7® Security Technical Implementation Overview, Version 1, Release 12. s.l. : Field Security Operations, Defense Information Systems Agency, 26 Jul 13.
3. Windows 8® Overview, Version 1, Release 2. s.l. : Field Security Operations, Defense Information Systems Agency, 26 Jul 13.
4. Enhanced Mitigation Experience Toolkit v3.0 User Guide. s.l. : Microsoft Corporation, 2012.

CONTACT INFORMATION

Industry Inquiries
410-854-6091
bao@nsa.gov

USG/IC Customer Inquiries
410-854-4790

DoD/Military/COCOM Customer Inquiries
410-854-4200

General Inquiries
NSA Information Assurance Service Center
niasc@nsa.gov